Practical Quantum Coin Flipping

Anna Pappa, Andre Chailloux, Eleni Diamanti, Iordanis Kerenidis

Practical Quantum Coin Flipping

Anna Pappa,[1,*] André Chailloux,[2,†] Eleni Diamanti,[1,‡] and Iordanis Kerenidis[2,§]

[1] *LTCI, CNRS - Télécom ParisTech, Paris, France*
[2] *LIAFA, CNRS - Université Paris 7, Paris, France*

(Dated: November 7, 2011)

We show that in the unconditional security model, a single quantum strong coin flip with security guarantees that are strictly better than in any classical protocol is possible to implement with current technology. Our protocol takes into account all aspects of an experimental implementation, including losses, multiphoton pulses emitted by practical photon sources, channel noise, detector dark counts, and finite quantum efficiency. We calculate the abort probability when both players are honest, as well as the probability of one player forcing his desired outcome. For a channel length up to 21 kmand commonly used parameter values, we can achieve honest abort and cheating probabilities that are better than in any classical protocol. Our protocol is, in principle, implementable using attenuated laser pulses, with no need for entangled photons or any other specific resources.

PACS numbers: 03.67.-a, 03.67.Dd

I. INTRODUCTION

Coin Flipping is a fundamental cryptographic primitive with numerous applications, where two distrustful parties separated by distance wish to agree on a random bit. There are two kinds of coin flipping: in *strong* coin flipping, the players wish to share a random bit without caring for a specific outcome, while in *weak* coin flipping, each player has a preference for one of the two values of the bit. A coin flipping protocol is called *fair* if the cheating probability for both players is the same.

Blum [1] introduced the first coin flipping protocol in 1981. This protocol is *asynchronous*, in the sense that the two players do not simultaneously send messages to each other but rather in communication rounds. In the asynchronous classical model, it is impossible to have a coin-flipping protocol with cheating probability less than 1, unless computational assumptions are considered. In other words, a dishonest player can always force the outcome of the coin flip with probability 1. On the other hand, in the *synchronous* (or *relativistic*) classical model [2], unconditionally secure coin flipping is possible, but the model itself is hard to implement because the security lies solely on the simultaneity of the communication and thus the verification of the distance between the two players.

In the quantum model, where the two parties share a quantum channel, the initial results for unconditionally secure coin flipping were discouraging. Lo and Chau [3] and Mayers [4] independently proved that quantum bit commitment is impossible and so is perfect quantum coin flipping. On the other hand, several quantum protocols have been proposed that achieve a cheating probability lower than 1. Aharonov *et al.* proposed the first such protocol [5], and other protocols followed [6–9] that nevertheless could not go below the cheating probability bound of 3/4. On the other hand, Kitaev [10], using semidefinite programming, proved that the cheating probability of any fair quantum coin flipping protocol is at least $1/\sqrt{2}$. Finally Chailloux and Kerenidis [11], using Mochon's result [12] for *weak* coin flipping with arbitrarily small bias, bridged the gap by presenting a protocol that has cheating probability arbitrarily close to $1/\sqrt{2}$.

These results are important from a theoretical point of view, however they assume perfect implementation of the protocols. The situation is more subtle when we deal with realistic conditions encountered in experimental implementations, for example multiphoton pulses emitted by practical sources, losses and channel noise, since if taken into account they may render protocols such as [5, 6, 11, 13, 14] completely unsecure in practice.

Recently, protocols that address some of the issues that arise in experimental implementations have been proposed. A major step was taken by Berlin *et al.* [15], who proposed a protocol that is completely impervious to losses and achieves a cheating probability of 0.9. In their theoretical analysis however, they do not deal with noise and thus the honest abort probability is always zero. This protocol becomes completely unsecure in the presence of multiphoton pulses, i.e. when the implementation is based on an attenuated laser source rather than a perfect single-photon source. Subsequently, Berlin *et al.* [16] implemented this protocol using a source of entangled qubits and hence avoiding multi-photon pulses. In order to deal with the noise present in the experiment, they defined a different primitive, *sequential coin flipping*, instead of a single coin flip, and conjectured that this primitive still remains impossible classically. Finally, based on [15], Chailloux [17] proposed an improved protocol with cheating probability 0.86, while Aharon et al [18] described a family of loss-tolerant protocols where for the case of two qubit, the cheating probability is 0,8975.

Barrett and Massar [19] state that, since there can be no error-correction in a single coin flip, there should be no quantum protocol that can tolerate noise and have a zero honest abort probability. To circumvent this diffi-

culty, they studied the primitive of *string coin flipping*, previously introduced by Kent [20], which was nevertheless proven to be possible classically.

II. OUR WORK

We present an unconditionally secure quantum strong coin flipping protocol that can be implemented using today's technology. Our goal is to take into account all experimental parameters, including noise, which forces us to allow some honest abort probability. We can then achieve both honest abort and cheating probability strictly smaller than in any classical protocol. Hänggi and Wullschleger [21] describe explicit classical and quantum protocols that achieve tight bounds for the cheating probability p, when the honest players abort with probability H. In the quantum case, the achievable bound is $p = \sqrt{(1-H)/2}$, and in the classical case, the achievable bound is equal to the quantum bound for $H \geq 1/2$, and $p = 1 - \sqrt{H/2}$ for $H < 1/2$.

Our protocol uses a standard attenuated laser source and we analyze how all practical aspects, like multi-photon pulses, channel noise, system loss, detector dark counts and finite quantum efficiency, affect the honest abort and cheating probability. We prove that for a single coin flip, if the noise is up to 2% and for channel length up to 21km, we can achieve at the same time honest abort probability ($\approx 1\%$) and cheating probability (≈ 0.93) strictly smaller than classically possible. We note that, similar to quantum key distribution protocols [22], our protocol is not completely impervious to losses, but can tolerate up to a certain amount of losses, which corresponds to distances in typical metropolitan area networks.

III. PROTOCOL

Our protocol is a refinement of the one proposed by Berlin et al [15]; the main difference is that Alice sends a fixed number of pulses K, and uses an attenuated laser source to produce her states instead of a perfect single-photon or an entangled-photon source. By restraining the number of pulses and by allowing an honest abort probability, the protocol can achieve a cheating probability very close to the one proven by Berlin et al, and at the same time be more suitable for practical use.

Each photon pulse produced by the source contains a number of photons that follows the Poisson distribution with $p_i = e^{-\mu}\mu^i/i!$ and mean photon number μ. The parameter a of the protocol is known from the start (we will later see how to optimize it).

1. For $i = 1, ..., K$:
   (a) Alice picks uniformly at random a basis $\alpha_i \in \{0,1\}$ and a bit $c_i \in \{0,1\}$.
   (b) She prepares the state $|\phi_{\alpha_i,c_i}\rangle$, such that:
   $$|\phi_{\alpha_i,0}\rangle = \sqrt{a}|0\rangle + (-1)^{\alpha_i}\sqrt{1-a}|1\rangle$$
   $$|\phi_{\alpha_i,1}\rangle = \sqrt{1-a}|0\rangle - (-1)^{\alpha_i}\sqrt{a}|1\rangle$$
   and sends it to Bob.
2. Bob picks uniformly at random a measurement basis α'_i for every pulse. If his detectors do not click for any pulse, then he aborts. Else, let j the first pulse he detects.
3. Bob picks uniformly at random $c'_j \in \{0,1\}$ and sends it to Alice, together with the index j.
4. Alice reveals α_j, c_j.
5. If $\alpha_j = \alpha'_j$, Bob checks that the outcome of his measurement is indeed $|\phi_{\alpha_j,c_j}\rangle$, otherwise he aborts.
6. If Bob has not aborted, then the outcome of the protocol is $b = c_j + c'_j$.

A. Honest Player Abort

Any amount of noise in an experimental implementation results in a non-zero honest abort probability. Here, we analyse exactly how noise and the other experimental parameters affect the honest abort probability in order to ensure that the protocol achieves a task which remains impossible classically. We note that a similar analysis can also be done for the Berlin *et al.* protocol. The situations in which an honest abort might occur with some probability are the following:

1. Bob's detectors do not click in any of the K rounds of the coin flip. The abort probability is 1.
2. Bob's first detection is due to a dark count. The abort probability is 1/4, since if $\alpha_j = \alpha'_j$ (step 5), he will abort with probability 1/2 (dark count is totally random), else if $\alpha_j \neq \alpha'_j$ he will not abort.
3. The noise in the channel alters the state of the photon. In this case, the abort probability is 1/2, since he will only abort if $\alpha_j = \alpha'_j$ (step 5).

The total honest abort probability is then:

$$H = Z^K(1-d_B)^K + \tfrac{1}{4}\textstyle\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i + \left[1 - Z^K(1-d_B)^K - \textstyle\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i\right]\frac{e}{2}$$

where $Z = p_0 + \big(1-p_0\big)\big(1-F\eta\big)$: probability that no signal arrives at Bob's detectors; F: system transmission efficiency; η: detector finite quantum efficiency; d_B: probability of detector dark count; e: probability of wrong measurement outcome due to noise, which can be due to imperfect state preparation, channel-induced operations and detector errors.

B. Malicious Alice

Alice's optimal cheating strategy in our protocol is the same as the one in the Berlin *et al.*'s protocol. We assume Alice to be all-powerful, which means that she controls all aspects of the implementation except Bob's measurement setup. It is in her best interest to replace the lossy channel with a perfect one, use a perfect single-photon source and send no vacuum states. We also assume that Bob's detectors are perfect, which only increases Alice's cheating probability and hence we provide an upper bound in this stronger security model. Under these assumptions, honest Bob will always succeed in measuring the first pulse that Alice sends and disregard the following ones. Hence, Alice's optimal cheating strategy is to create some entangled state, send one qubit to Bob in the first pulse, wait for Bob to reply in step 3 and then perform some measurement in her part of the entangled state in order to decide what to reveal in step 4. This is no different from the cheating in Berlin et al's protocol, so the optimal cheating probability for Alice is $p_A \leq \big(3+2\sqrt{a(1-a)}\big)/4$ [15].

C. Malicious Bob

We consider Bob to be all powerful, meaning that he controls all aspects of the implementation, except for Alice's photon source. Again, it is in Bob's best interest to replace the lossy and noisy channel with a perfect one, in order to receive each time the correct state and maximize his cheating probability. Moreover, we assume he has perfect detectors and we also give him the ability to know the number of photons in each of the K pulses. Then, Bob's optimal strategy is to receive all K pulses and then perform some operation on the received qubits in order to maximize his information about Alice's bit c_j for some pulse j. It is important to note that honest Alice picks a new uniformly random bit c_j for each pulse j and hence Bob cannot combine different pulses in order to increase his information about a bit c_j.

To simplify our analysis, we assume that in the case where Bob has received at least two two-photon pulses or a pulse with 3 or more photons, then he can cheat with probability 1. We analyze the following events (in each event, the remaining pulses contain zero photons):

A_1 : (all zero-photon pulses) The optimal cheating strategy for Bob is to pick a random bit.

A_2 : (at least one one-photon pulse) The optimal cheating strategy for Bob is to measure in the computational basis (Helstrom measurement)[15, 23]. It is proven in [15] that this probability is equal to a.

A_3 : (one two-photon pulse) It can be proven that for our states the optimal measurement in a two-photon pulse outputs the correct bit with probability equal to a.

A_4 : (one two-photon pulse, at least one 1-photon pulse) Bob will try to benefit from the two-photon pulse (see discussion below), and if he fails, he will continue like in A_2, since the pulses are independent.

We denote as b' Bob's desired outcome and as $P(b'|A_i)$ the probability that Bob will force his preference when event A_i has taken place. We get an upper bound for the total probability of cheating Bob:

$$p_B \;\leq\; \sum_{i=1}^{4} P(A_i) \times P(b'|A_i) + \left[1 - \sum_{i=1}^{4} P(A_i)\right] \times 1$$

Note that an honest Alice prepares the K pulses independently, which means that a measurement on any of them does not affect the rest. Consequently, Bob can measure each pulse independently, without affecting the remaining pulses. Moreover, the probability for each of these events depends on the protocol parameter K and on the mean photon number μ (which is controlled by Alice).

It remains to bound $P(b'|A_4)$, i.e. the case where Bob has received one 2-photon pulse and some single photon pulses. Bob will try to profit from the two identical quantum states in one pulse. On one hand, he can perform the optimal distinguishing measurement on the two photons, which as we said earlier gives a correct answer with probability a. On the other hand, he can perform a conclusive measurement on the 2-photon pulse that with some probability will give a correct answer and with some probability will give no answer at all (in which case Bob can use one of the 1-photon pulses). In fact, none of these two strategies is optimal. In general, Bob will perform some measurement that with probability c will provide an answer, which will be correct with probability γ, and with probability $(1-c)$ the measurement will provide no answer, in which case Bob will use a single-photon pulse to guess correctly with probability a. Hence,

$$P(b'|A_4) = \max_M\{c\gamma + (1-c)a\}$$

over all possible measurements of Bob.

Let M be the optimal measurement that provides with probability c an answer that is correct with probability γ and with probability $(1-c)$ provides an answer that is correct with probability γ'. On one hand, we have that $\gamma' \geq 1/2$ (since Bob can always guess with probability $1/2$) and on the other hand this measurement cannot be correct with probability larger than a (since we know that the optimal measurement has probability a). Hence, we have $x \equiv c\gamma + (1-c)1/2 \leq a$ from which we get that $c \geq 2x - 1$. Then, we have:

$$\begin{aligned} P(b'|A_4) = c\gamma + (1-c)a \;&\leq\; x + (2-2x)(a - \tfrac{1}{2}) \\ &\leq\; -2a^2 + 4a - 1 \end{aligned} \qquad (1)$$

Equation (1) provides an analytical upper bound on the cheating probability for event A_4 and hence we can now calculate the cheating probability p_B.

Finally to ensure the fairness of the protocol, we adjust a so that $p_A = p_B$ in order to have equal cheating probabilities.

IV. RESULTS

We have introduced a strong coin flipping protocol that takes into account all experimental parameters. In the following simulations, we use parameter values commonly referenced in the literature [24, 25], which can be implemented using today's technology.

The photon signals that Alice sends arrive with a probability F (transmission efficiency) at Bob's site, and they are detected with a probability η (detector quantum efficiency). For an optical channel, F is related to the channel absorption coefficient β, the channel length L and a distance-independent constant loss k, via the equation: $F = 10^{-(\beta L+k)/10}$. The values used in our simulations are shown in the following table.

Parameter		Value
Receiver constant loss [dB]	k	1
Absorption coefficient [dB/km]	β	0.2
Detection efficiency	η	0.2
Dark counts (per slot)	d_B	10^{-5}
Signal error rate	e	0.01

Note that we consider the probability of a signal and a dark count occurring simultaneously negligible.

Our protocol requires a minimum honest abort probability equal to half of the probability of noise in the channel. We consider an acceptable honest abort probability smaller than 2%, thus by setting the honest abort probability to fixed values up to 0.02 for different channel lengths, we find the necessary rounds K and the optimal mean photon number μ that minimize the cheating probability for a fair protocol.

There is an inversely proportional relation between the honest abort probability and the optimal μ (Figure 1). The same holds for the number of rounds K in relation to the honest abort probability and for the same μ. When μ is increased in order to achieve the desired honest abort probability, the required number of rounds is reduced. The number of rounds K depends on the honest abort probability and ranges between 2000 and 15000.

In Figure 2 we plot our protocol's cheating probability versus the honest abort probability H for four different channel lengths, and compare this to the optimal classical cheating probability, which is equal to $1 - \sqrt{H/2}$ [21].

For any length up to 21 km and honest abort probability smaller than 2%, we can find a μ such that the maximum cheating probability of our protocol is better than in the classical case. Figure 3 shows how the coefficient a of the protocol states changes in relation to the honest abort probability, for three different channel lengths.

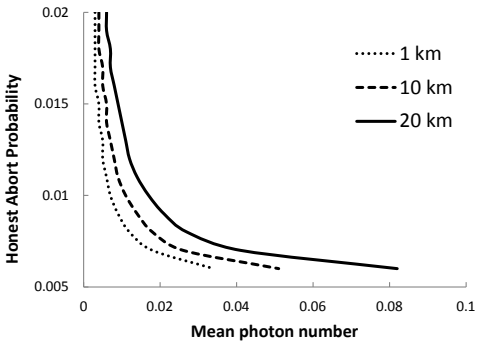

Figure 1: Quantum honest abort probability vs mean photon number μ for different channel lengths.

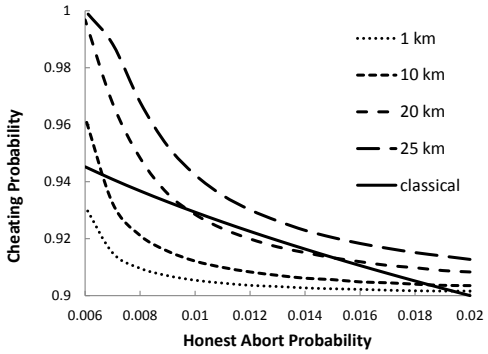

Figure 2: Quantum honest abort vs cheating probability for different channel lengths and comparison to the classical case.

V. DISCUSSION

We have shown that flipping a single coin with security guarantees that are strictly stronger than in any classical protocol can be achieved with present quantum technology, and more precisely with a standard attenuated laser source. This implies that quantum information can be used beyond quantum key distribution (QKD), to achieve in practice more difficult cryptographic tasks in a model where the parties do not trust each other. We note that implementations of such tasks will be subject to the same

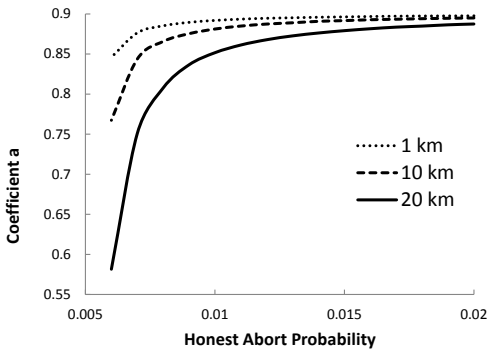

Figure 3: Quantum state coefficient vs honest abort probability.

issues related to the existence of side channels as in QKD (eg. [26]).

We observe that the maximal communication distance that can be achieved is significantly smaller than in QKD [22]. In principle, we cannot expect to have the same results as in QKD, since the setting is much harder. Here, the adversary is the other player, so no cooperation is possible, thus excluding error-correction and privacy amplification. With the parameter values that we used, the limit to the channel length is 21 km. We can increase the channel length by improving the experimental parameters, in particular the signal error rate.

Even though Chailloux [17] proposed a protocol with lower cheating probability than the Berlin *et al.*, it does not perform as well in the presence of noise.

Last, it is interesting to see if there is a way to reduce the effect of noise to the honest abort probability with current technology. We note that this seems hard, since any attempt of Alice to protect the qubits, via a repetition error correcting code for example, will immediately increase the cheating probability of Bob.

Acknowlegments – We acknowledge financial support from the ANR through projects CRYQ (ANR-09-JCJC-0067-01), FREQUENCY (ANR-09-BLAN-0410-01), and QRAC (ANR-08-EMER-012), and from the European Union through project QCS (grant 255961).

* Electronic address: anna.pappa@telecom-paristech.fr
† Electronic address: andre.chailloux@lri.fr
‡ Electronic address: eleni.diamanti@telecom-paristech.fr
§ Electronic address: jkeren@liafa.jussieu.fr

[1] M. Blum, in *ECE Report 82-04* (1981), pp. 11.
[2] A. Kent, *Phys. Rev. Lett.* **83**, 5382 (1999).
[3] H.-K. Lo and H. F. Chau, *Physica D* **120**, 177 (1998).
[4] D. Mayers, *Phys. Rev. Lett.* **78**, 3414 (1997).
[5] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao, in *Proceedings of STOC* (2000), pp. 705–714.
[6] A. Ambainis, *Journal of Computer and System Sciences* **68**, 398 (2004).
[7] R. Spekkens and T. Rudolph, *Phys. Rev. Lett.* **89**, 227901 (2002).
[8] R. Colbeck, *Phys. Rev. A* **362**, 390 (2007).
[9] A. Nayak and P. Shor, *Phys. Rev. A* **67**, 012304 (2003).
[10] A. Kitaev, Presentation at the 6th workshop on quantum information processing, QIP 2003, MSRI, Berkeley, CA.
[11] A. Chailloux and I. Kerenidis, 50^{th} Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), October 25-27, 2009, Atlanta.
[12] C. Mochon, in *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science* (FOCS 04), pp. 2–11, Washington, DC, USA, 2004. IEEE Computer Society.
[13] G. Molina-Terriza, A. Vaziri, R. Urzin, and A. Zeilinger, *Phys. Rev. Lett.* **94**, 040501 (2005).
[14] A. T. Ngyuen, J. Frison, K. P. Huy, and S. Massar, *New Journal of Physics* **10**, 083087 (2008).
[15] G. Berlin, G. Brassard, F. Bussières, and N. Godbout, *Phys. Rev. A* **80**, 062321 (2009).
[16] G. Berlin, G. Brassard, F. Bussières, N. Godbout, J. Slater, and W. Tittel, e-print arXiv:0904.3946v2[quant-ph] (2009).
[17] A. Chailloux, e-print arXiv:1009.0044v3[quant-ph] (2010).
[18] N. Aharon, S. Massar, and J. Silman, *Phys. Rev. A* **82**, 052307 (2010).
[19] J. Barrett and S. Massar, *Phys. Rev. A* **69**, 022322 (2004).
[20] A. Kent, in *Proceedings of the 6^{th} International Conference on Quantum Communication, Measurement and Computing*, QCMC'02 (Rinton Press Inc, 2003).
[21] E. Hänggi and J. Wullschleger, in *Proceedings of the 8^{th} Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011*, Lecture Notes in Computer Science, Vol. 6597 (Springer, 2011) (2010).
[22] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
[23] C. Helstrom, J. Stat. Phys. **1**, 231 (1969).
[24] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).
[25] N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (2000).
[26] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Nature Photonics* **4**, 686 (2010).